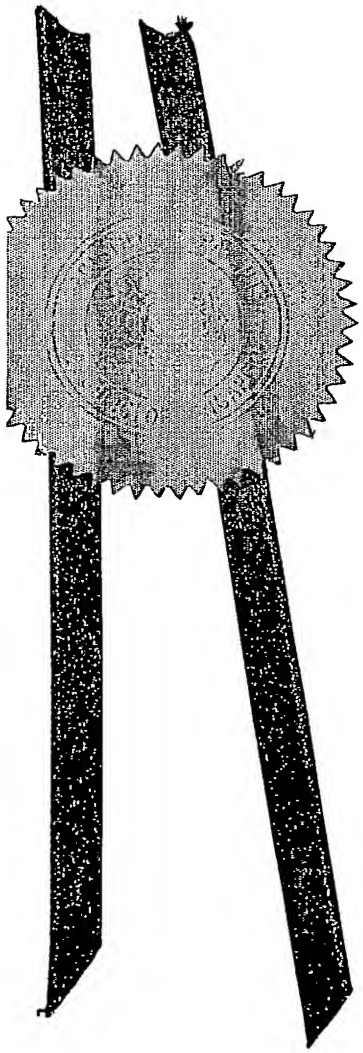
SG 10/502005
227

**REGISTRY OF PATENTS**
**SINGAPORE**

This is to certify that the annexed is a true copy of the following PCT international application as filed in this Registry.



| | | |
|---|---|---|
| Date of Filing | : | 31 JULY 2002 (31-07-2002) |
| Application number | : | PCT/SG02/00171 |
| Applicants | : | TREK 2000 INTERNATIONAL LTD |
| Title of Invention | : | SYSTEM AND METHOD FOR AUTHENTICATION |



**Serene Chan** (Miss)
Assistant Registrar
For Registrar of Patents
Singapore

27 August 2003

*192192*

*G00002*

# PCT

HOME COPY

## REQUEST

The undersigned requests that the present international application be processed according to the Patent Cooperation Treaty.

For receiving Office use only

PCT/SG 02/00171

International Application No.

31 JUL 2002 (31-07-2002)

International Filing Date

REGISTRY OF PATENTS (SINGAPORE)
PCT INTERNATIONAL APPLICATION

Name of receiving Office and "PCT International Application"

Applicant's or agent's file reference *(if desired) (12 characters maximum)*: FP1726

**Box No. I TITLE OF INVENTION**

SYSTEM AND METHOD FOR AUTHENTICATION

**Box No. II APPLICANT** ☐ This person is also inventor

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

Trek 2000 International Ltd
30 Loyang Way #07-13/14/15
Loyang Industrial Estate
Singapore 508769

Telephone No.

Facsimile No.

Teleprinter No.

Applicant's registration No. with the Office

State *(that is, country)* of nationality: Singapore

State *(that is, country)* of residence: Singapore

This person is applicant for the purposes of: ☐ all designated States ☒ all designated States except the United States of America ☐ the United States of America only ☐ the States indicated in the Supplemental Box

**Box No. III FURTHER APPLICANT(S) AND/OR (FURTHER) INVENTOR(S)**

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

OOI Chin Shyan
Blk 438 Tampines St. 43 #08-157
Singapore 520438

This person is:
☐ applicant only
☒ applicant and inventor
☐ inventor only *(If this check-box is marked, do not fill in below.)*

Applicant's registration No. with the Office

State *(that is, country)* of nationality: Malaysia

State *(that is, country)* of residence: Singapore

This person is applicant for the purposes of: ☐ all designated States ☐ all designated States except the United States of America ☒ the United States of America only ☐ the States indicated in the Supplemental Box

☒ Further applicants and/or (further) inventors are indicated on a continuation sheet.

**Box No. IV AGENT OR COMMON REPRESENTATIVE; OR ADDRESS FOR CORRESPONDENCE**

The person identified below is hereby/has been appointed to act on behalf of the applicant(s) before the competent International Authorities as: ☒ agent ☐ common representative

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country.)*

WATKIN, Timothy Lawrence Harvey
Lloyd Wise
Tanjong Pagar P O Box 636
Singapore 910816

Telephone No.
65 6227 8986

Facsimile No.
65 6227 3898

Teleprinter No.

Agent's registration No. with the Office

☐ **Address for correspondence:** Mark this check-box where no agent or common representative is/has been appointed and the space above is used instead to indicate a special address to which correspondence should be sent.

**Continuation of Box No. III** **FURTHER APPLICANT(S) AND/OR (FURTHER) INVENTOR(S)**

*If none of the following sub-boxes is used, this sheet should not be included in the request.*

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

LIM Lay Chuan
Blk 322 Bukit Batok St. 33 #03-04
Singapore 650322

This person is:
- ☐ applicant only
- ☒ applicant and inventor
- ☐ inventor only *(If this check-box is marked, do not fill in below.)*

Applicant's registration No. with the Office

State *(that is, country)* of nationality: Malaysia

State *(that is, country)* of residence: Singapore

This person is applicant for the purposes of: ☐ all designated States ☐ all designated States except the United States of America ☒ the United States of America only ☐ the States indicated in the Supplemental Box

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

POO Teng Pin
Blk 44 Bedok South Road #11-763
Singapore 460044

This person is:
- ☐ applicant only
- ☒ applicant and inventor
- ☐ inventor only *(If this check-box is marked, do not fill in below.)*

Applicant's registration No. with the Office

State *(that is, country)* of nationality: Malaysia

State *(that is, country)* of residence: Singapore

This person is applicant for the purposes of: ☐ all designated States ☐ all designated States except the United States of America ☒ the United States of America only ☐ the States indicated in the Supplemental Box

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

This person is:
- ☐ applicant only
- ☐ applicant and inventor
- ☐ inventor only *(If this check-box is marked, do not fill in below.)*

Applicant's registration No. with the Office

State *(that is, country)* of nationality:

State *(that is, country)* of residence:

This person is applicant for the purposes of: ☐ all designated States ☐ all designated States except the United States of America ☐ the United States of America only ☐ the States indicated in the Supplemental Box

Name and address: *(Family name followed by given name; for a legal entity, full official designation. The address must include postal code and name of country. The country of the address indicated in this Box is the applicant's State (that is, country) of residence if no State of residence is indicated below.)*

This person is:
- ☐ applicant only
- ☐ applicant and inventor
- ☐ inventor only *(If this check-box is marked, do not fill in below.)*

Applicant's registration No. with the Office

State *(that is, country)* of nationality:

State *(that is, country)* of residence:

This person is applicant for the purposes of: ☐ all designated States ☐ all designated States except the United States of America ☐ the United States of America only ☐ the States indicated in the Supplemental Box

☐ Further applicants and/or (further) inventors are indicated on another continuation sheet.

**Box No. V DESIGNATION OF STATES** *Mark the applicable check-boxes below; at least one must be marked.*

The following designations are hereby made under Rule 4.9(a):

**Regional Patent**

- ☒ AP **ARIPO Patent:** GH Ghana, GM Gambia, KE Kenya, LS Lesotho, MW Malawi, MZ Mozambique, SD Sudan, SL Sierra Leone, SZ Swaziland, TZ United Republic of Tanzania, UG Uganda, ZW Zimbabwe, and any other State which is a Contracting State of the Harare Protocol and of the PCT
- ☒ EA **Eurasian Patent:** AM Armenia, AZ Azerbaijan, BY Belarus, KG Kyrgyzstan, KZ Kazakhstan, MD Republic of Moldova, RU Russian Federation, TJ Tajikistan, TM Turkmenistan, and any other State which is a Contracting State of the Eurasian Patent Convention and of the PCT
- ☒ EP **European Patent:** AT Austria, BE Belgium, CH & LI Switzerland and Liechtenstein, CY Cyprus, DE Germany, DK Denmark, ES Spain, FI Finland, FR France, GB United Kingdom, GR Greece, IE Ireland, IT Italy, LU Luxembourg, MC Monaco, NL Netherlands, PT Portugal, SE Sweden, TR Turkey, and any other State which is a Contracting State of the European Patent Convention and of the PCT
- ☒ OA **OAPI Patent:** BF Burkina Faso, BJ Benin, CF Central African Republic, CG Congo, CI Côte d'Ivoire, CM Cameroon, GA Gabon, GN Guinea, GW Guinea-Bissau, ML Mali, MR Mauritania, NE Niger, SN Senegal, TD Chad, TG Togo, and any other State which is a member State of OAPI and a Contracting State of the PCT *(if other kind of protection or treatment desired, specify on dotted line)* .....

**National Patent** *(if other kind of protection or treatment desired, specify on dotted line)*:

| | | |
|---|---|---|
| ☒ AE United Arab Emirates | ☒ GH Ghana | ☒ MX Mexico |
| ☒ AG Antigua and Barbuda | ☒ GM Gambia | ☒ MZ Mozambique |
| ☒ AL Albania | ☒ HR Croatia | ☒ NO Norway |
| ☒ AM Armenia | ☒ HU Hungary | ☒ NZ New Zealand |
| ☒ AT Austria | ☒ ID Indonesia | ☒ PL Poland |
| ☒ AU Australia | ☒ IL Israel | ☒ PT Portugal |
| ☒ AZ Azerbaijan | ☒ IN India | ☒ RO Romania |
| ☒ BA Bosnia and Herzegovina | ☒ IS Iceland | ☒ RU Russian Federation |
| ☒ BB Barbados | ☒ JP Japan | |
| ☒ BG Bulgaria | ☒ KE Kenya | ☒ SD Sudan |
| ☒ BR Brazil | ☒ KG Kyrgyzstan | ☒ SE Sweden |
| ☒ BY Belarus | ☒ KP Democratic People's Republic of Korea | ☒ SG Singapore |
| ☒ BZ Belize | | ☒ SI Slovenia |
| ☒ CA Canada | ☒ KR Republic of Korea | ☒ SK Slovakia |
| ☒ CH & LI Switzerland and Liechtenstein | ☒ KZ Kazakhstan | ☒ SL Sierra Leone |
| ☒ CN China | ☒ LC Saint Lucia | ☒ TJ Tajikistan |
| ☒ CO Colombia | ☒ LK Sri Lanka | ☒ TM Turkmenistan |
| ☒ CR Costa Rica | ☒ LR Liberia | ☒ TR Turkey |
| ☒ CU Cuba | ☒ LS Lesotho | ☒ TT Trinidad and Tobago |
| ☒ CZ Czech Republic | ☒ LT Lithuania | |
| ☒ DE Germany | ☒ LU Luxembourg | ☒ TZ United Republic of Tanzania |
| ☒ DK Denmark | ☒ LV Latvia | ☒ UA Ukraine |
| ☒ DM Dominica | ☒ MA Morocco | ☒ UG Uganda |
| ☒ DZ Algeria | ☒ MD Republic of Moldova | ☒ US United States of America |
| ☒ EC Ecuador | | |
| ☒ EE Estonia | ☒ MG Madagascar | ☒ UZ Uzbekistan |
| ☒ ES Spain | ☒ MK The former Yugoslav Republic of Macedonia | ☒ VN Viet Nam |
| ☒ FI Finland | | ☒ YU Yugoslavia |
| ☒ GB United Kingdom | ☒ MN Mongolia | ☒ ZA South Africa |
| ☒ GD Grenada | ☒ MW Malawi | ☒ ZW Zimbabwe |
| ☒ GE Georgia | | |

Check-boxes below reserved for designating States which have become party to the PCT after issuance of this sheet:

| | | |
|---|---|---|
| ☒ PH Philippines | ☒ ZM Zambia | ☐ |
| ☒ OM Oman | ☒ TN Tunisia | ☐ |

**Precautionary Designation Statement:** In addition to the designations made above, the applicant also makes under Rule 4.9(b) all other designations which would be permitted under the PCT except any designation(s) indicated in the Supplemental Box as being excluded from the scope of this statement. The applicant declares that those additional designations are subject to confirmation and that any designation which is not confirmed before the expiration of 15 months from the priority date is to be regarded as withdrawn by the applicant at the expiration of that time limit. *(Confirmation (including fees) must reach the receiving Office within the 15-month time limit.)*

**Box No. VI PRIORITY CLAIM**

The priority of the following earlier application(s) is hereby claimed:

| Filing date of earlier application *(day/month/year)* | Number of earlier application | Where earlier application is: | | |
|---|---|---|---|---|
| | | national application: country | regional application:* regional Office | international application: receiving Office |
| item (1) | | | | |
| item (2) | | | | |
| item (3) | | | | |
| item (4) | | | | |
| item (5) | | | | |

☐ Further priority claims are indicated in the Supplemental Box.

The receiving Office is requested to prepare and transmit to the International Bureau a certified copy of the earlier application(s) *(only if the earlier application was filed with the Office which for the purposes of this international application is the receiving Office)* identified above as:

☐ all items ☐ item (1) ☐ item (2) ☐ item (3) ☐ item (4) ☐ item (5) ☐ other, see Supplemental Box

* *Where the earlier application is an ARIPO application, indicate at least one country party to the Paris Convention for the Protection of Industrial Property or one Member of the World Trade Organization for which that earlier application was filed (Rule 4.10(b)(ii)):* ....

.....

**Box No. VII INTERNATIONAL SEARCHING AUTHORITY**

**Choice of International Searching Authority (ISA)** *(if two or more International Searching Authorities are competent to carry out the international search, indicate the Authority chosen; the two-letter code may be used)*:

ISA / AT .....

**Request to use results of earlier search; reference to that search** *(if an earlier search has been carried out by or requested from the International Searching Authority)*:

Date *(day/month/year)* Number Country *(or regional Office)*

**Box No. VIII DECLARATIONS**

The following declarations are contained in Boxes Nos. VIII (i) to (v) *(mark the applicable check-boxes below and indicate in the right column the number of each type of declaration)*: Number of declarations

| | | |
|---|---|---|
| ☐ Box No. VIII (i) | Declaration as to the identity of the inventor | : |
| ☐ Box No. VIII (ii) | Declaration as to the applicant's entitlement, as at the international filing date, to apply for and be granted a patent | : |
| ☐ Box No. VIII (iii) | Declaration as to the applicant's entitlement, as at the international filing date, to claim the priority of the earlier application | : |
| ☐ Box No. VIII (iv) | Declaration of inventorship (only for the purposes of the designation of the United States of America) | : |
| ☐ Box No. VIII (v) | Declaration as to non-prejudicial disclosures or exceptions to lack of novelty | : |

**Box No. IX CHECK LIST; LANGUAGE OF FILING**

This international application contains:

(a) the following number of sheets in paper form:

| | | |
|---|---|---|
| request (including declaration sheets) | : | 5 |
| description (excluding sequence listing part) | : | 13 |
| claims | : | 4 |
| abstract | : | 1 |
| drawings | : | 6 |
| **Sub-total number of sheets** | : | 29 |
| sequence listing part of description *(actual number of sheets if filed in paper form, whether or not also filed in computer readable form; see (b) below)* | : | |
| **Total number of sheets** | : | 29 |

(b) sequence listing part of description filed in **computer readable form**

(i) ☐ only (under Section 801(a)(i))

(ii) ☐ in addition to being filed in paper form (under Section 801(a)(ii))

**Type and number of carriers** (diskette, CD-ROM, CD-R or other) on which the sequence listing part is contained *(additional copies to be indicated under item 9(ii), in right column)*: .....

| This international application is accompanied by the following item(s) *(mark the applicable check-boxes below and indicate in right column the number of each item)*: | Number of items |
|---|---|
| 1. ☒ fee calculation sheet | 1 |
| 2. ☐ original separate power of attorney | |
| 3. ☐ original general power of attorney | |
| 4. ☐ copy of general power of attorney; reference number, if any: ..... | |
| 5. ☐ statement explaining lack of signature | |
| 6. ☐ priority document(s) identified in Box No. VI as item(s): ..... | |
| 7. ☐ translation of international application into *(language)*: ..... | |
| 8. ☐ separate indications concerning deposited microorganism or other biological material | |
| 9. ☐ sequence listing in computer readable form (indicate also type and number of carriers (diskette, CD-ROM, CD-R or other)) | |
| (i) ☐ copy submitted for the purposes of international search under Rule 13*ter* only (and not as part of the international application) | |
| (ii) ☐ *(only where check-box (b)(i) or (b)(ii) is marked in left column)* additional copies including, where applicable, the copy for the purposes of international search under Rule 13*ter* | |
| (iii) ☐ together with relevant statement as to the identity of the copy or copies with the sequence listing part mentioned in left column | |
| 10. ☒ other *(specify)*: PF48 ..... | 1 |

**Figure of the drawings which should accompany the abstract:** 1

**Language of filing of the international application:** English

**Box No. X SIGNATURE OF APPLICANT, AGENT OR COMMON REPRESENTATIVE**

*Next to each signature, indicate the name of the person signing and the capacity in which the person signs (if such capacity is not obvious from reading the request).*

Timothy Watkin

WATKIN, Timothy Lawrence Harvey
Agent for the Applicant

**For receiving Office use only**

1. Date of actual receipt of the purported international application: 31 JUL 2002 (31-07-2002)

2. Drawings:
☒ received:
☐ not received:

3. Corrected date of actual receipt due to later but timely received papers or drawings completing the purported international application:

4. Date of timely receipt of the required corrections under PCT Article 11(2):

5. International Searching Authority (if two or more are competent): ISA / AT

6. ☐ Transmittal of search copy delayed until search fee is paid

**For International Bureau use only**

Date of receipt of the record copy by the International Bureau:

# SYSTEM AND METHOD FOR AUTHENTICATION

## Background of the Invention

### 1. Field of the Invention

The present invention relates generally to digital and software piracy. More particularly, the present invention relates to a system and a method for authentication to prevent piracy in a digital system.

### 2. Description of the Related Art

The piracy and illegal copying of software and other digital media has become extremely pervasive and currently results in billions of dollars in lost revenue for media and software owners worldwide. This problem is compounded by the advent of faster and more technologically advanced computers, the development of inexpensive mass storage media (*i.e.* CDs, DVDs), as well as copying devices such as CD writers, which aid in various aspects of digital piracy.

Each technological breakthrough seemingly results in a new and better way to illegally copy intellectual property belonging to another. Examples of digital piracy include: the copying of proprietary software to sell to others, the installing of a single proprietary software package on several different systems, placing a copy of proprietary software on the Internet, or even downloading copyrighted images from the Internet.

While digital piracy is fairly common among many end users who have lawfully purchased the software, large-scale piracy typically occurs at a reseller level. For instance, a reseller may duplicate and distribute multiple copies of a software program, a digital audio file or a digital video file to different customers. These counterfeit versions are sometimes passed on to unsuspecting customers. Hardware distributors have been known to preload different systems using a single software package. In such

instances, customers are either not provided with original manuals, diskettes and/or compact discs (CDs) or are simply supplied with pirated copies of the same.

Numerous methods to combat the rampant problem of digital piracy have been devised. One of the methods is the use of trialware to restrict usage of a software product. Trialware may be implemented by either programming an expiration date or a usage counter into a software program. Such a scheme limits the use of a software product to a particular duration or a number of trial times, respectively, after which the protected application can no longer be launched. Users are then forced to either purchase the full version of the product or to quit using it altogether.

Hardware keys are another type of anti-piracy device that is commonly used to prevent illegal use of software. Hardware keys are devices that are plugged into selected ports of a computer. Once the software is executed, it then detects the presence of a hardware key in a similar manner to detecting other hardware devices (such as a printer, monitor or a mouse). Programming the software such that it only operates when an appropriate hardware key is attached prevents illegal use of the software. As the number of hardware keys distributed to end users correspond to the number of seat licenses purchased, the software will not work when installed on another system without the requisite hardware key.

Another common anti-piracy technique is to require the entry of a certain registration key that is supplied by the software company before the software can be installed. Traditionally, the registration keys are given only with the original software package, although some are issued electronically. Unfortunately, there is nothing to prevent the holder of the registration key from installing the software on multiple systems. In addition, many of the electronic registration keys are based on the user's personal information (*i.e.* such as the user's name), therefore, some hackers have developed programs to calculate registration keys for random names.

Unfortunately, as with the use of the registration key, all of the above anti-piracy systems (and many others) are easily circumvented by hackers. A common method of combating these anti-piracy techniques is to disassemble the coding of the Application

Programming Interface (API) to assembly language and, thereafter, decompile the assembly language into programming language. With the knowledge gained from the program flow, the hacker can easily re-write the program or set certain conditions within the program itself, such that it bypasses all the anti-piracy authentication algorithms.

In view of the foregoing, it is extremely desirable to have an anti-piracy system that cannot be easily re-programmed or bypassed by computer hackers and other digital pirates. It is also desirable to have an anti-piracy system that can be integrated with existing mass storage devices.

## Summary of the Invention

The present invention fills these needs by providing a system and a method for authentication in a digital system. It should be appreciated that the present invention can be implemented in numerous ways, including as a process, an apparatus, a system, a device or a method. Several inventive embodiments of the present invention are described below.

In one embodiment of the present invention, an authentication system to verify a password from a host is provided. The authentication system includes a first storage unit to store an authentication sequence and a read-only memory unit on which an authentication algorithm is programmed. The authentication sequence is preferably encrypted or hash-coded. A microcontroller is coupled to the first storage unit, the read-only memory unit and the host. The microcontroller receives the password and executes the authentication algorithm to verify the password with the authentication sequence. Access to a second storage unit is permitted by the microcontroller only if the password has been verified. Data that is to be written onto or read from the second storage unit is preferably encrypted, respectively. Alternatively, the data may be hash-coded.

The read-only memory unit preferably includes a shutdown algorithm to shut down the host and the authentication system when a series of incorrect passwords is received by the microcontroller. The first storage unit, the microcontroller, the read-only memory unit, and the second storage unit are preferably implemented on a single chip. In addition,, it is also a preference to have the first storage unit and the read-only memory unit incorporated into the microcontroller.

In a preferred embodiment of the present invention, the authentication algorithm is implemented on either firmware or hardware. The first storage unit is preferably located within the read-only memory unit and the authentication sequence is preferably hard code into the authentication algorithm. Alternatively, the first storage unit may be located within the second storage device.

In another embodiment of the present invention, a method for authenticating a password is provided. The method begins by providing an authentication sequence and receiving the password. An authentication algorithm, stored on a read-only memory unit, is executed to verify the password with the authentication sequence. Access to a storage unit is permitted only if the password is verified. Preferably, a new password is re-entered if the password is not verified. It is also preferable to shut down the entire system if a series of wrong passwords is received. Data that is to be written onto or read from the storage unit is preferably encrypted or decrypted respectively. Alternatively, the data may be hash-coded.

Other aspects and advantages of the invention will become apparent from the following detailed description, taken in conjunction with the accompanying drawings, illustrating by way of example the principles of the invention.

## Brief Description of the Drawings

The present invention will be readily understood by the following detailed description in conjunction with the accompanying drawings. To facilitate this description, like reference numerals designate like structural elements.

Figure 1 illustrates a schematic of an authentication system to verify a password from a host in accordance with one embodiment of the present invention.

Figure 2 illustrates a schematic of an authentication system to verify a password from a host in accordance with a further embodiment of the present invention.

Figure 3 illustrates a schematic of an authentication system to verify a password from a host in accordance with another embodiment of the present invention.

Figure 4 illustrates a schematic of an authentication system to verify a password from a host in accordance with yet another embodiment of the present invention.

Figure 5 illustrates a method for authenticating a password from a host in accordance with one embodiment of the present invention.

Figure 6 illustrates a schematic of a computer system using an anti-piracy file manager in accordance with a further embodiment of the present invention.

## Detailed Description of the Preferred Embodiments

A system and a method for authentication in a digital system are provided. In the following description, numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be understood, however, to one skilled in the art, that the present invention may be practiced without some or all of these specific details. In other instances, well known process operations have not been described in detail in order not to unnecessarily obscure the present invention.

Figure 1 illustrates an authentication system 10 to verify a password 12 from a host 14 in accordance with one embodiment of the present invention. Authentication system 10 includes a first storage unit 16, a read-only memory (ROM) unit 18 and a microcontroller 20. Microcontroller 20 is coupled to host 14, first storage unit 16, ROM unit 18 and a second storage unit 22. Microcontroller 20 is preferably coupled to host 14 through a USB controller.

In other embodiments of the present invention, ROM unit 18 may be formed as part of microcontroller 20. Furthermore, both first storage unit 16 and second storage unit 22 may be one of a number of mass storage devices, including hard drives, floppy disks, or removable flash memory devices, such as the ThumbDrive manufactured by Trek 2000. In addition, the two storage units may be utilized in one physical structure to form a single mass storage device. The mass storage device may also be placed with microcontroller 20 to form a single chip.

First storage unit 16 stores an authentication sequence 24, which is used to verify password 12. An authentication algorithm 26 to authenticate password 12 with authentication sequence 24 is programmed onto ROM unit 18. In addition, ROM unit 18 preferably comprises a shutdown algorithm 28. Because these algorithms and other data are hard coded, the contents of ROM unit 18 cannot be decompiled or altered. Upon receiving password 12, microcontroller 20 loads and executes authentication algorithm 26 to verify password 12 with authentication sequence 24. Access to second storage unit 22 is permitted only if password 12 is verified.

Password 12 may be entered by a user or a software program executed by host 14 after receiving a query from microcontroller 20. Because authentication algorithm 26 is hard coded onto ROM unit 18, copying or decompiling and changing the software program resident on host 14 does not breach the copy protection provided by the present invention. It will be apparent to one skilled in the art that password 12 may be a private string of characters, a sequence of communication protocols or some other security protocol known only to an authorized user. In addition, password 12 and authentication sequence 24 may form part of a biometric authentication process by using a user's fingerprints, iris, face, or voice as authentication means.

Password 12 may also be programmed into the software running on host 14 and recognizable only by authentication algorithm 26 and therefore not known to an end user. As described above, authentication algorithm 26 is preferably implemented on hardware or firmware (such as ROM unit 18) so that it is tamper resistant; that is, authentication algorithm 26 will be either extremely difficult to reverse engineer or extract data from, and therefore extremely difficult to bypass.

Shutdown algorithm 28 is preferably implemented as a deterrent against brute force attacks by shutting down the entire system if a series of incorrect passwords is received by microcontroller 20. An authentication system programmer may define the maximum number of incorrect passwords allowed before the system shuts down. Shutdown algorithm 28 may also be programmed to not accept anymore password entries for a specified amount of time. By using shutdown algorithm 28, trial and error methods used by brute force application programs to identify password 12 would become an extremely tedious process for hackers. The algorithm would therefore deter potential hackers from even attempting to identify password 12.

Second storage unit 22 is used to store programs and/or files, which are required for a program on host 12 to run. Examples of such files include executable programs (such as a software installer), digital audio files, digital video files, image files, text files, and library files. Microcontroller 20 allows access to second storage unit 22 from host 14 only if the correct password 12 has been received by microcontroller 20.

Although illustrated in this embodiment as separate entities, it should be evident to a person skilled in the art that microcontroller 20, first storage unit 16, ROM unit 18 and second storage unit 22 may be combined in a number of ways. For example, microcontroller 20, first storage unit 16, ROM unit 18 and second storage unit 22 may be implemented on a single semiconductor chip. In an alternative embodiment, microcontroller 20 and ROM unit 18 may be implemented on a chip that is separate from the storage units.

The present invention therefore has great flexibility of design that may easily be altered depending on a user's requirements. For example, on one hand, the use of multiple chips may allow different vendors to manufacture different parts of the authentication system. On the other hand, fabricating the present invention onto fewer chips (or a single chip) may be less expensive and provide better performance. In addition, if ROM unit 18 and microcontroller 20 are located on the same chip, it may be more difficult to separate the ROM to read the data stored.

Figure 2 illustrates an authentication system 50 to verify a password 52 from a host 54 in accordance with a further embodiment of the present invention. Authentication system 50 comprises a first storage unit 56, a ROM unit 58 and a microcontroller 60. Microcontroller 60 is coupled to host 54, first storage unit 56, ROM unit 58 and an encoder 62. Encoder 62 is further coupled to a second storage unit 64. First storage unit 56 stores an authentication sequence 66, which is used to verify password 52. An authentication algorithm 68 to authenticate password 52 is programmed onto ROM unit 58. ROM unit 58 preferably includes a shutdown algorithm 70.

Upon receiving password 52, microcontroller 60 loads and executes authentication algorithm 68 to verify password 52 with authentication sequence 66. Access to second storage unit 64 is permitted only if password 52 is verified. Shutdown algorithm 70 preferably shuts down the entire system if a series of wrong passwords is received by microcontroller 60. An authentication system programmer determines the maximum number of incorrect password attempts allowed.

Data to be read from or written onto second storage unit 64 is first decrypted or encrypted respectively by encoder 62. Many different encryption schemes may be used by encoder 62, including International Data Encryption Algorithm (IDEA), Data Encryption Standard (DES) encryption, Triple Data Encryption Standard (3-DES) encryption, and Pretty Good Privacy (PGP). By encrypting the contents of second storage unit 64, a hacker will not be able to make sense of the contents even if he manages to read the contents bypassing microcontroller 60 (for example, by using a probe). After password 52 has been authenticated, a decoder (not illustrated) may be used to decrypt the contents of second storage unit 64.

Alternatively, the data stored in second storage unit 64 may be protected by hash-coding. In addition, authentication sequence 66 is preferably encrypted or hashed as well to prevent hackers from unraveling authentication sequence 66. This may be accomplished without requiring an additional encoder if first storage unit 56 is located within second storage unit 64.

Figure 3 illustrates a schematic of an authentication system 100 to verify a password 102 from a host 104 in accordance with another embodiment of the present invention. Authentication system 100 comprises a ROM unit 106 and a microcontroller 108. Microcontroller 108 is coupled to host 104, ROM unit 106 and an encoder 110. Encoder 110 is further coupled to a storage unit 112. An authentication algorithm 114 to authenticate password 102 is programmed onto ROM unit 106. An authentication sequence 116 to verify password 102 is hard code into authentication algorithm 114. ROM unit 106 preferably comprises a shutdown algorithm 118.

As described in previous embodiments, upon receiving password 102, microcontroller 108 loads and executes authentication algorithm 114 to verify password 102 with authentication sequence 116. Access to storage unit 112 is permitted only if password 102 is verified. Shutdown algorithm 118 is preferably used to shut down the entire system if a series of incorrect passwords is received by microcontroller 108.

By hard coding authentication sequence 116 directly into authentication algorithm 114, possibly in multiple places, modification of authentication sequence 116

becomes substantially more difficult. In order to change a hard code authentication sequence, not only is recompilation necessary (if using a compiled language), but also sufficient understanding of the implementation is required to ensure that the change will not cause program failure. Such a measure makes it difficult for a hacker to re-program authentication system 100.

Figure 4 illustrates an authentication system 150 to verify a password 152 from a host 154 in accordance with another embodiment of the present invention. Authentication system 150 comprises a read-only memory (ROM) unit 156 and a microcontroller 158. Microcontroller 158 is coupled to host 154, ROM unit 156 and an encoder 160. Encoder 160 is further coupled to a storage unit 162. Data to be read from or written onto storage unit 162 is first decrypted or encrypted respectively by encoder 160. Alternatively, hash-coding may be employed to protect the data stored in storage unit 162.

Storage unit 162 is made up of two types of data storage areas: a public storage area 164 and a private storage area 166. An authentication sequence 168, which is used to verify password 152, is stored in private storage area 166. An authentication algorithm 170 to authenticate password 152 is programmed onto ROM unit 156. ROM unit 156 also contains a shutdown algorithm 172. Public storage area 164 and private storage area 166 may be created by under-declaring the memory size available on storage unit 162.

Take for example a storage unit with physical addresses ranging from 000 to 1000, if only physical addresses 000 to 500 are declared to an operating system (OS) such as Windows, on host 154, the OS will not be aware of the presence of physical addresses 501 to 1000. Under such circumstances, data stored within physical addresses 000 to 500 will be accessible to any user. This area is known as a public storage area. Conversely, the undeclared physical addresses 501 to 1000 form a private storage area since these addresses are only be available to microcontroller 158 and can only be accessed by an authorized user or software program.

Under non-secure operating conditions, any user may instruct host 154 to read data from or write data onto public storage area 164. However, if a user wishes to access private storage area 166, the user or the software program must first enter password 152, which is then sent to microcontroller 158 for authentication. Upon receiving password 152, microcontroller 158 executes authentication algorithm 170 to verify password 152 with authentication sequence 168. Access to private storage area 166 is permitted only if password 152 is verified. Shutdown algorithm 172 shuts down the entire system if a series of incorrect passwords is received by microcontroller 158.

Figure 5 illustrates a method 200 for authenticating a password from a host in accordance with one embodiment of the present invention. An authentication sequence is first provided in a block 202 and preferably stored in a first storage unit. Also provided, in another block 204, is an authentication algorithm, which is stored in a ROM unit. After receiving a prompt from the host, a password is entered in by a user or by a software program. The password is then received in a block 206 by a microcontroller that executes an authentication algorithm to verify the password with the authentication sequence in a decision block 208.

If the password is verified in decision block 208, access to a private area, such as the second storage unit in the above-described embodiments, will be permitted in a block 210. The user is then able to read from or write onto the second storage unit, which is preferably encrypted. If the password is not verified in decision block 208, the user will be denied access to the second storage unit and method 200 will end in a block 212. Alternatively, if the password is incorrect, the user may be given additional chances to enter the right password. However, system is preferably shut down if a series of incorrect passwords is received by the microcontroller.

Figure 6 illustrates a schematic of a computer system 250 using an anti-piracy file manager 252 in accordance with a further embodiment of the present invention. Anti-piracy file manager 252 is coupled to an anti-piracy authentication engine 254 and a storage unit 256. Anti-piracy manager 252 answers requests from a number of software programs 258 that request different authentication schemes from anti-piracy authentication engine 254. Access to storage unit 256 is guarded by an authentication

system 260. In this exemplary system, the flexibility of the present invention allows for authentication of many different types of software programs at the same time through anti-piracy file manager 252.

Other embodiments of the invention will be apparent to those skilled in the art from consideration of the specification and practice of the invention. Furthermore, certain terminology has been used for the purposes of descriptive clarity, and not to limit the present invention. The embodiments and preferred features described above should be considered exemplary, with the invention being defined by the appended claims.

## CLAIMS

1. An authentication system to verify a password from a host, comprising:

a first storage unit to store an authentication sequence;

a read-only memory unit, wherein said read-only memory unit is to store an authentication algorithm;

a microcontroller coupled to said first storage unit, said read-only memory unit, and said host, wherein said microcontroller is to receive said password and execute said authentication algorithm and wherein said authentication algorithm is to verify said password with said authentication sequence; and

a second storage unit coupled to said microcontroller, wherein access to said second storage unit is permitted by said microcontroller only if said password has been verified.

2. An authentication system to verify a password from a host as recited in claim 1, wherein said read-only memory unit further comprises a shutdown algorithm to shut down said host and said authentication system after a number of incorrect passwords is received by said microcontroller.

3. An authentication system to verify a password from a host as recited in claim 2, wherein said password is a private string of characters.

4. An authentication system to verify a password from a host as recited in claim 2, wherein said password is a sequence of communication protocols.

5. An authentication system to verify a password from a host as recited in claim 1, wherein said authentication algorithm is hard coded on one of a group consisting of a firmware and a hardware in said microcontroller.

6. An authentication system to verify a password from a host as recited in claim 5, wherein said second storage unit is a removable storage device.

7. An authentication system to verify a password from a host as recited in claim 6, wherein said second storage unit uses flash memory.

8. An authentication system to verify a password from a host as recited in claim 1, wherein said microcontroller and said read-only memory unit are implemented on a single semiconductor chip.

9. An authentication system to verify a password from a host as recited in claim 8, wherein said first storage unit and said read-only memory unit are incorporated into said microcontroller.

10. An authentication system to verify a password from a host as recited in claim 1, further comprising an encoder coupled between said microcontroller and said second storage unit, wherein said encoder is to encrypt data that is to be written onto said second storage unit.

11. An authentication system to verify a password from a host as recited in claim 10, further comprising a decoder coupled between said microcontroller and said second storage unit, wherein said decoder is to decrypt data that is to be read from said second storage unit.

12. An authentication system to verify a password from a host as recited in claim 11, wherein data stored in said second storage unit is hash-coded.

13. An authentication system to verify a password from a host as recited in claim 12, wherein said authentication sequence is encrypted.

14. An authentication system to verify a password from a host as recited in claim 12, wherein said authentication sequence is hash-coded.

15. An authentication system to verify a password from a host as recited in claim 1, wherein said first storage unit is located within said read-only memory unit and wherein said authentication sequence is hard coded into said first storage unit.

16. An authentication system to verify a password from a host as recited in claim 15, wherein said second storage area further comprises a public storage area and a private storage area.

17. An authentication system to verify a password from a host as recited in claim 16, wherein said first storage unit is located within said private storage area of said second storage area.

18. A method for authenticating a password, comprising:

providing an authentication sequence;

receiving said password;

executing an authentication algorithm to verify said password with said authentication sequence, wherein said authentication algorithm is stored on a read-only memory unit; and

permitting access to a storage unit only if said password is verified.

19. A method for authenticating a password as recited in claim 18, further comprising encrypting data to be written onto said storage area.

20. A method for authenticating a password as recited in claim 19, further comprising decrypting data to be read from said storage area.

21. A method for authenticating a password as recited in claim 18, further comprising receiving a new password if said password is not verified.

22. A method for authenticating a password as recited in claim 21, further comprising shutting down a system if a series of incorrect passwords is received.

# SYSTEM AND METHOD FOR AUTHENTICATION


## Abstract

An authentication system to verify a password from a host is provided. The authentication system includes a first storage unit to store an authentication sequence and a read-only memory unit on which an authentication algorithm is programmed. A microcontroller is coupled to the first storage unit, the read-only memory unit and the host. The microcontroller receives the password and executes the authentication algorithm to verify the password with the authentication sequence. Access to a second storage unit is permitted by the microcontroller only if the password has been verified.


Figure 1

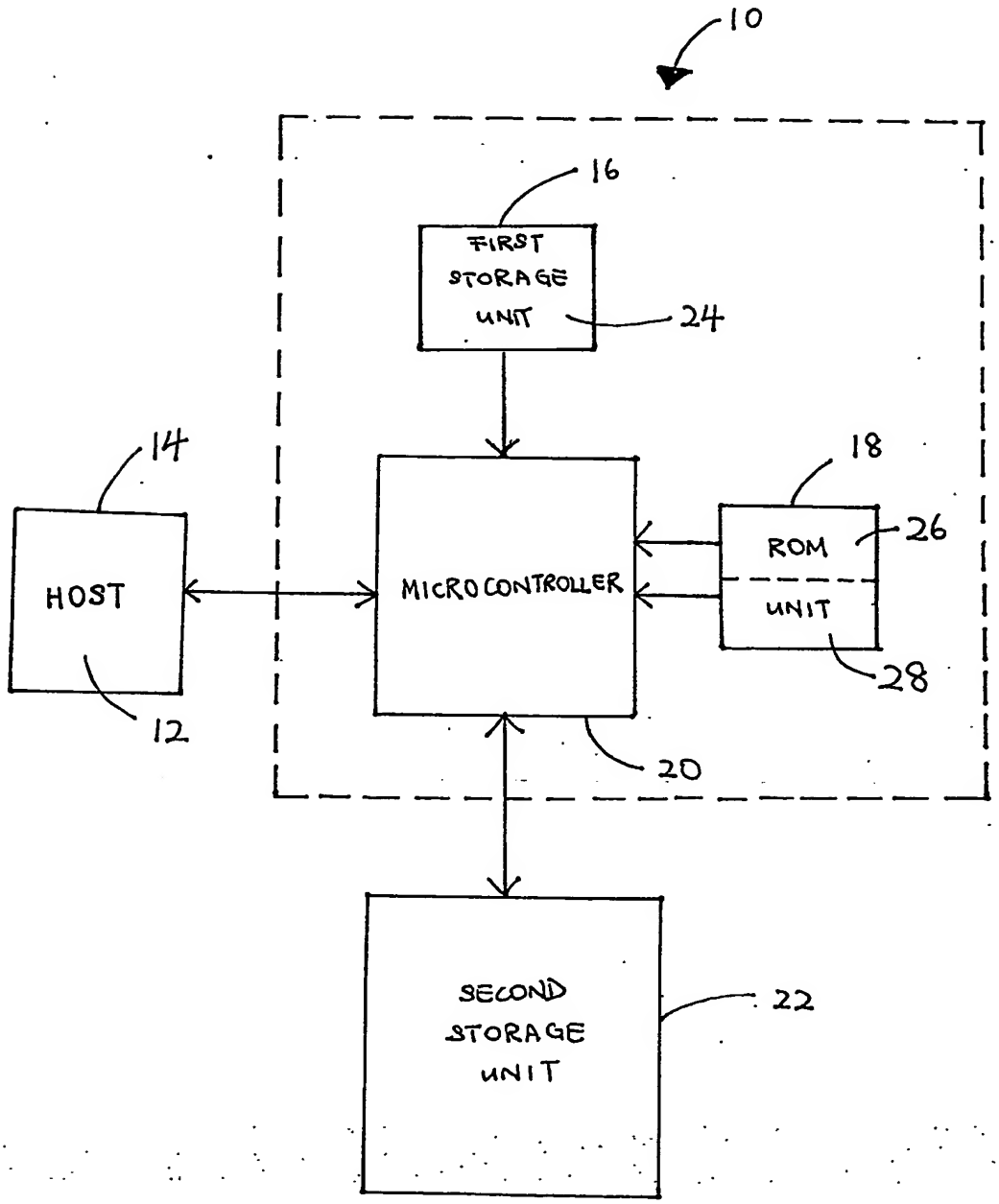

10
16
FIRST STORAGE UNIT
24
14
18
HOST
MICRO CONTROLLER
ROM
26
UNIT
28
12
20
SECOND STORAGE UNIT
22

Figure 1

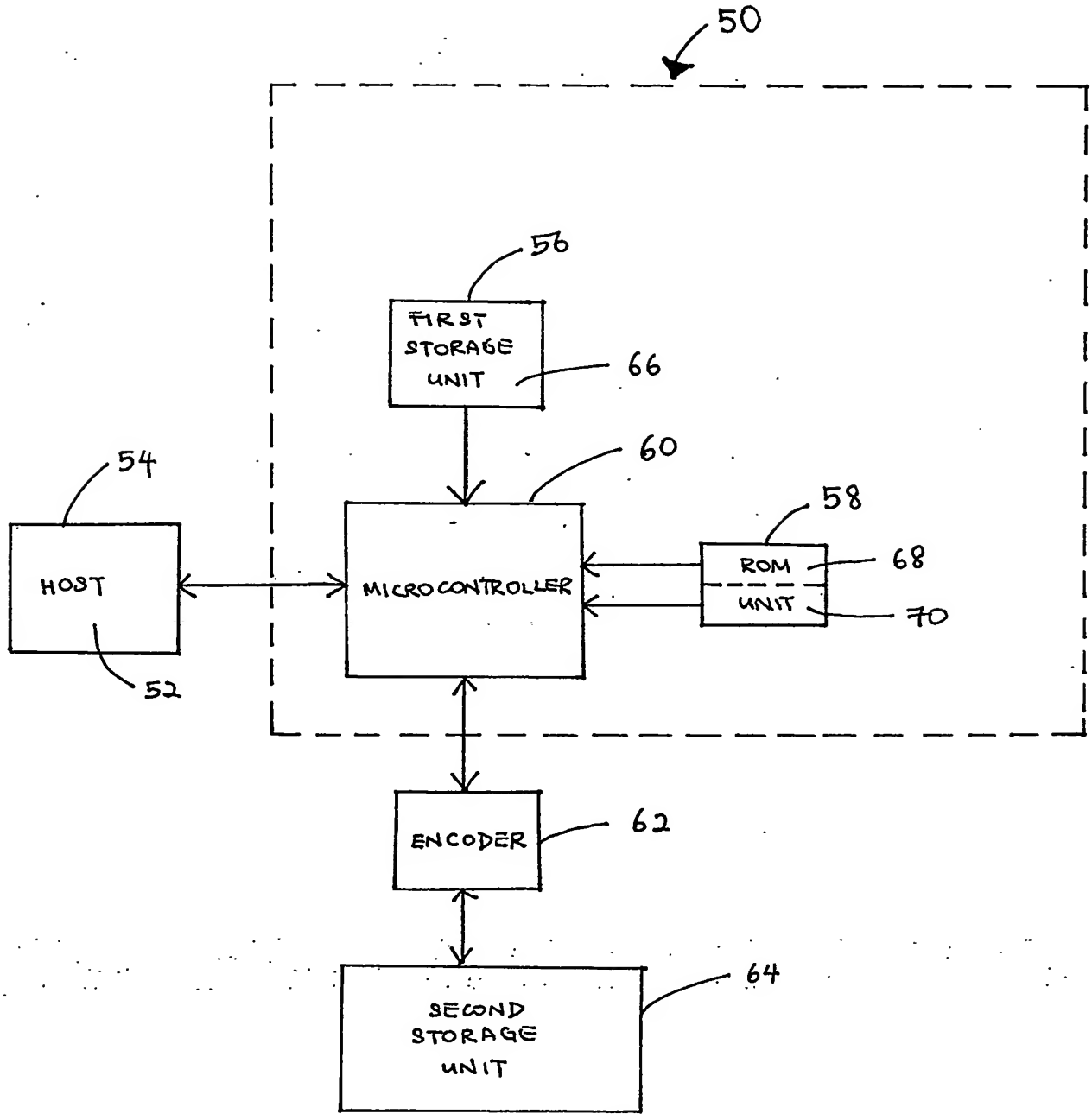

50
56
FIRST STORAGE UNIT
66
54
60
58
HOST
MICROCONTROLLER
ROM UNIT
68
70
52
ENCODER
62
64
SECOND STORAGE UNIT

Figure 2

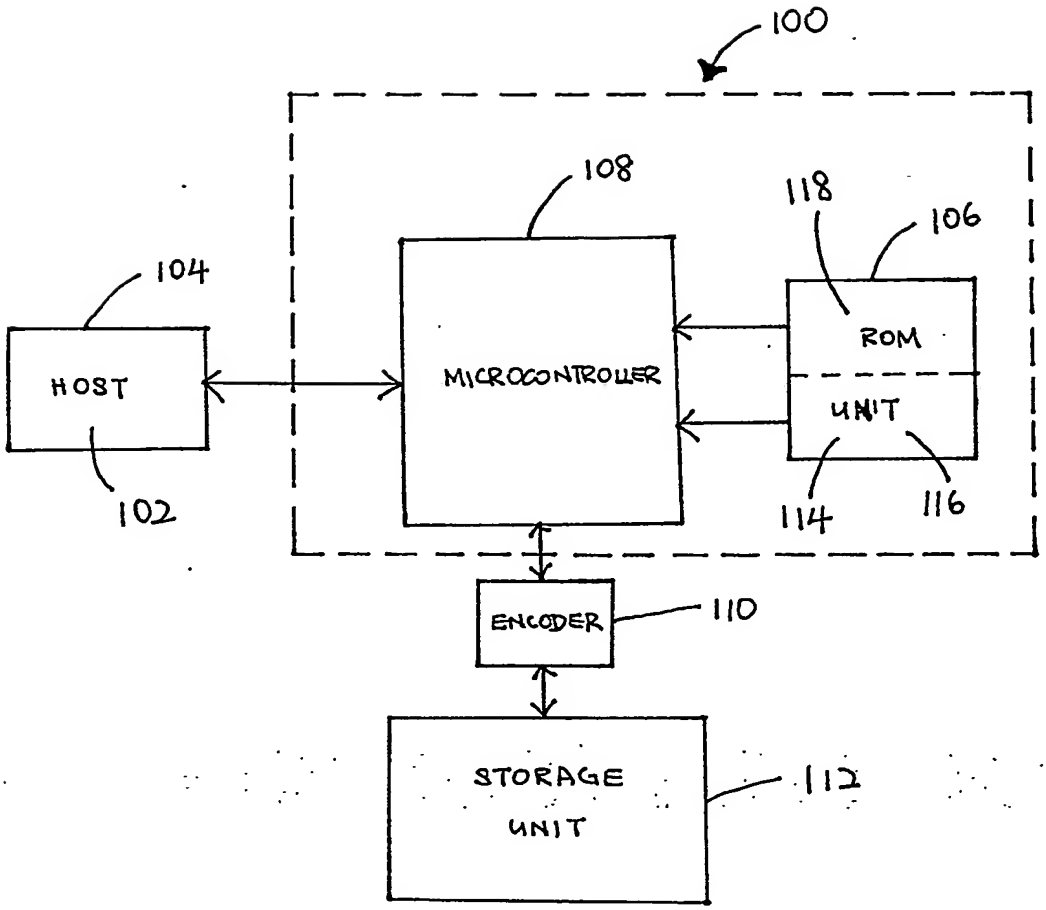

100
108
118
106
104
HOST
MICROCONTROLLER
ROM
UNIT
102
114
116
ENCODER
110
STORAGE
UNIT
112

Figure 3

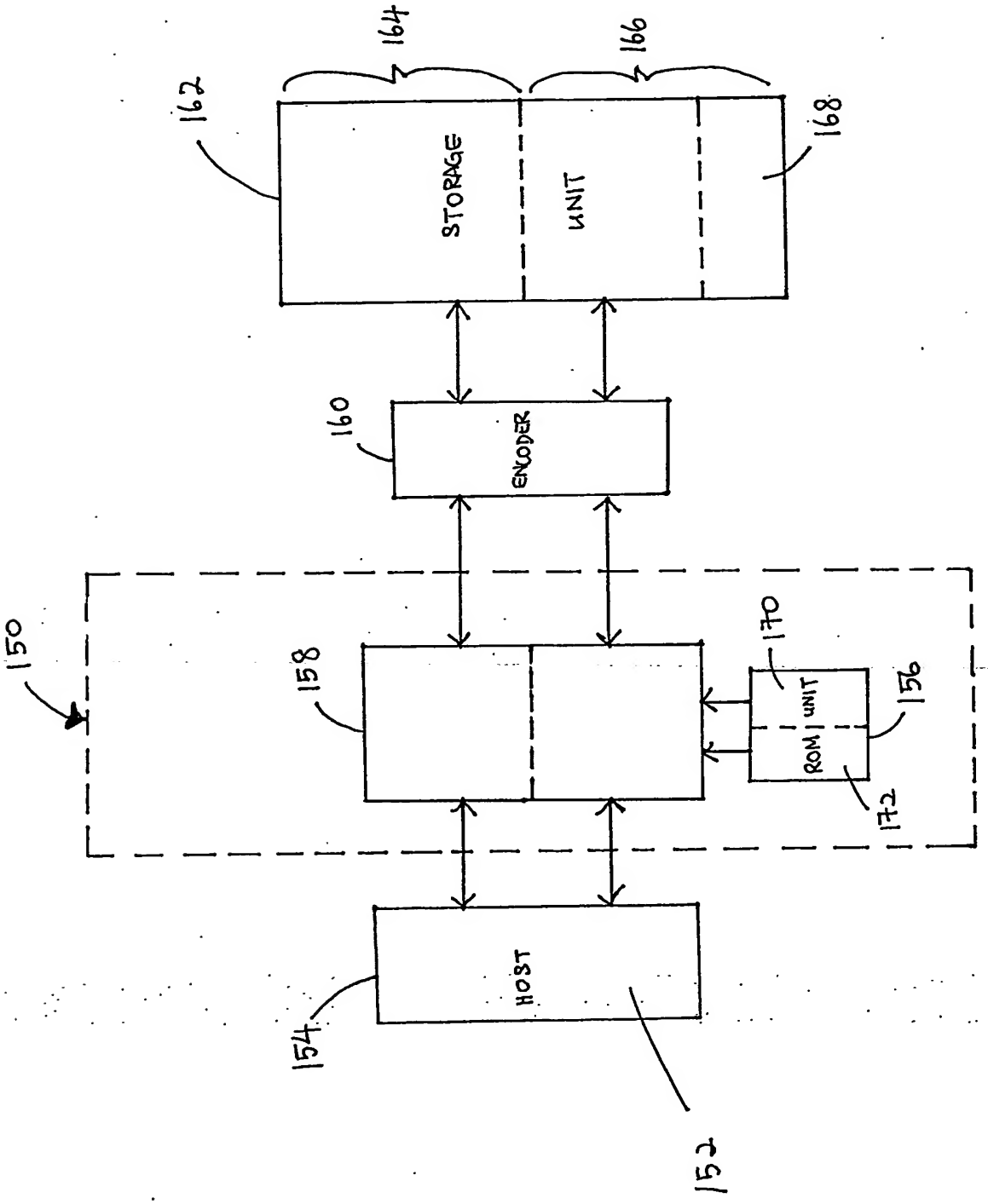

164
166
162
168
STORAGE
UNIT
160
ENCODER
150
158
170
ROM UNIT
156
172
HOST
154
152

Figure 4

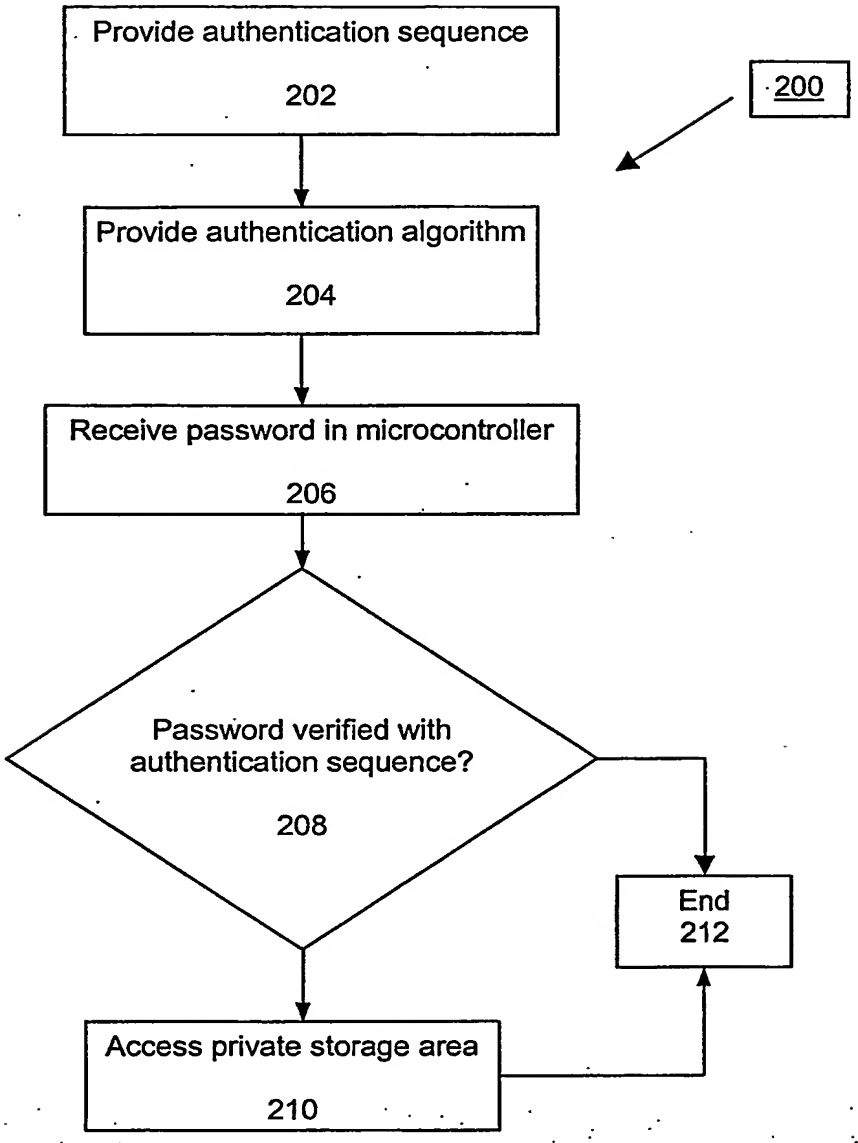

Provide authentication sequence
202
200
Provide authentication algorithm
204
Receive password in microcontroller
206
Password verified with authentication sequence?
208
End
212
Access private storage area
210

Figure 5

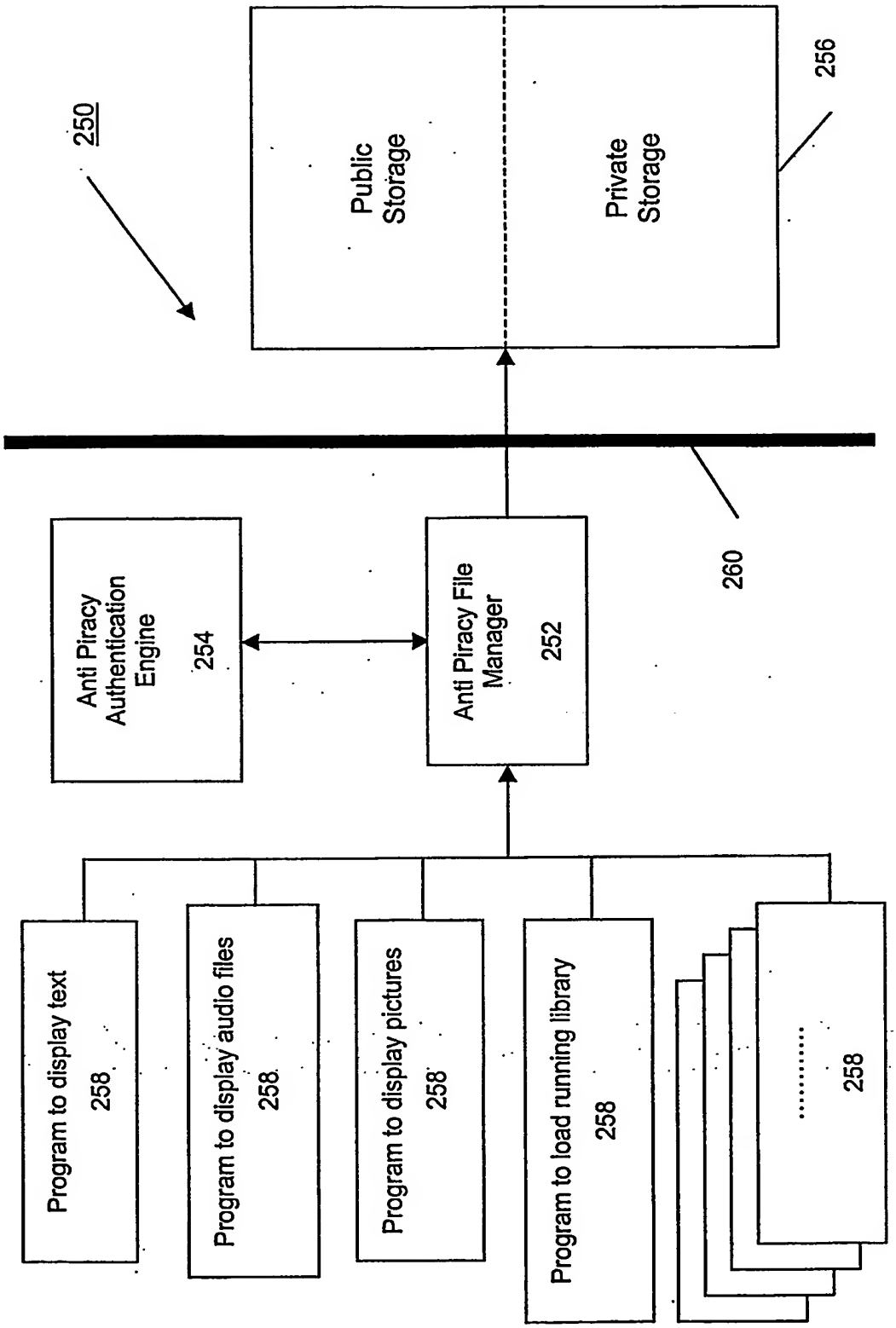

250
Public Storage
Private Storage
256
260
Anti Piracy Authentication Engine
254
Anti Piracy File Manager
252
Program to display text
258
Program to display audio files
258
Program to display pictures
258
Program to load running library
258
.....
258

Figure 6